Designs, Codes and Cryptography (2020) 88:1273–1284
https://doi.org/10.1007/s10623-020-00745-8

Relative generalized Hamming weights of affine Cartesian codes

Mrinmoy Datta[1]

Received: 11 September 2019 / Revised: 20 February 2020 / Accepted: 21 February 2020 /
Published online: 10 March 2020

Abstract
We explicitly determine all the relative generalized Hamming weights of affine Cartesian codes using the notion of footprints and results from extremal combinatorics. This generalizes the previous works on the determination of relative generalized Hamming weights of Reed–Muller codes by Geil and Martin, as well as the determination of all the generalized Hamming weights of the affine Cartesian codes by Beelen and Datta.

Keywords Affine Cartesian codes · Relative generalized Hamming weights · Footprint bounds

Mathematics Subject Classification 11T71 · 06A07 · 14G50 · 94B27

1 Introduction

Determination of parameters of Reed–Muller type codes has received a lot of attention from several mathematicians in recent past. In this paper, we look at a certain class of codes, called the affine Cartesian codes, that comes naturally as a generalization of Reed–Muller Codes. These codes were introduced in 2013 by Geil and Thomsen [12] in a more general setting of weighted Reed–Muller codes. The name "affine Cartesian codes" was coined by López et al. [17] in 2014. Since then several articles have appeared where the parameters of these codes were studied extensively. Like in the case of Reed–Muller codes, the problem of computing parameters such as minimum distance, generalized Hamming weights etc., of affine Cartesian codes translates to the problem of determination of the maximum number of common zeroes of systems of polynomials satisfying certain properties in a subset of an affine space over a finite field. The fundamental properties of affine Cartesian codes, such as their dimensions

Communicated by J. Jedwab.

Mrinmoy Datta is supported by a postdoctoral fellowship from DST-RCN Grant INT/NOR/RCN/ICT/P-03/2018.

✉ Mrinmoy Datta
mrinmoy.dat@gmail.com

[1] Institute of Mathematics and Statistics, University of Tromsø, Tromsø, Norway

and the minimum distances, were obtained in [17]. Later in 2018, the generalized Hamming weights [1] of the affine Cartesian codes were completely determined. This generalizes the classical work [15] of Heijnen and Pellikaan towards the determination of all the generalized Hamming weights of the Reed–Muller codes. Several articles, for example [3,4], are devoted towards the determination of the next to minimal weights of affine Cartesian codes.

The notion of generalized Hamming weights of a code was introduced by Wei [21] in 1991 in order to characterize the code performance of on a wire tap channel of type II. A generalization of these weights is known as the relative generalized Hamming weight of a code C_1 with respect to a proper subcode C_2. This notion was introduced by Luo et al. [18], again towards studying new characters on the wire tap channel of type II, in 2005 and was further studied in a subsequent article [16] by Liu et al. For the definition of the relative generalized Hamming weights of linear codes we refer to Sect. 2.1.

As the title of the article indicates, we are interested in determining the relative generalized Hamming weights of an affine Cartesian code with respect to a subcode which is again an affine Cartesian code. This work generalizes the result in the article [11] where the authors have determined all the relative generalized Hamming weights of the Reed–Muller codes. Also, the main results of the current article can be viewed as a generalization of the result in [1] which gives all the generalized Hamming weights of affine Cartesian codes. In proving our result in this paper, we follow the footsteps of [1] and [11], where the results were derived using the notion of the so-called footprint bound. Some early articles on footprint bounds include [8,10,14] and some recent articles include [2,13,20] among others. A somewhat brief discussion of the notion of the footprint bounds is given in Sect. 2.3.

The paper is organized as follows. In Sect. 2, we recall most of the definitions and the known results that will be used in proving our main theorem. In Sect. 3, we deduce Theorem 3.7, which can be viewed as an extension of the famous Kruskal–Katona Theorem in extremal combinatorics. Finally, in Sect. 4, we state and prove the main result of the paper where we compute all the relative generalized Hamming weights of an affine Cartesian code with respect to a smaller affine Cartesian code.

2 Preliminaries

We devote this section to recalling the well-known definitions and results that will be used in the sequel. In particular, we recall the definitions of relative generalized Hamming weights of a code with respect to a smaller subcode and the notion of affine Cartesian codes in the following two subsections. Later, we revisit the notion of the so called footprint bound which helps us in translating the algebraic geometric problem of determination of the maximum number of common zeroes of certain systems of polynomials in a specified subset of the affine space over a projective space into a seemingly different problem in extremal combinatorics. We will conclude this section by introducing some combinatorial notations which will be used in the next section. In particular, none of the results or definitions mentioned in this section are new. For more detailed description of the results that are mentioned here a reader is encouraged to see the references mentioned and the references therein.

2.1 Relative generalized Hamming weights of linear codes

We begin this subsection by recalling the definition of the relative generalized Hamming weights of a code with respect to a proper subcode. Throughout, we will denote by $\mathbb{F}_q$ a finite field with q elements where q is a prime power.

Definition 2.1 [16, Definition 2] Let $C_2 \subsetneq C_1$ be linear codes and $\ell := \dim C_1 - \dim C_2$. For $r = 1, \ldots, \ell$, the r-th *relative generalized Hamming weights* of C_1 with respect to C_2 (RGHW of C_1 w.r.t. C_2) is defined as

$$M_r(C_1, C_2) := \min_{J \subseteq \{1,\ldots,n\}} \{|J| : \dim((C_1)_J) - \dim((C_2)_J) = r\},$$

where $(C_i)_J = \{c = (c_1, \ldots, c_n) \in C_i \mid c_t = 0 \text{ for } t \notin J\}$ for $i = 1, 2$. The sequence $(M_1(C_1, C_2), \ldots, M_\ell(C_1, C_2))$ is known as the hierarchy of RGHWs of C_1 w.r.t. C_2.

The following Lemma, which can be found as [16, Lemma 1], gives an alternative definition of the RGHWs of a code C_1 w.r.t. a proper subcode C_2.

Lemma 2.2 [16, Lemma 1] *Let $C_2 \subsetneq C_1$ be linear codes and $\ell = \dim C_1 - \dim C_2$. For $r = 1, \ldots, \ell$, we have*

$$M_r(C_1, C_2) = \min \{|\mathrm{Supp}(D)| : D \subset C_1; D \cap C_2 = \{0\}, \dim D = r\}, \tag{1}$$

where, given a subspace D of $\mathbb{F}_q^n$, the support of D, denoted by $\mathrm{Supp}(D)$*, is given by*

$$\mathrm{Supp}(D) := \{i \in \{1, \ldots, n\} \mid c_i \neq 0 \text{ for some } (c_1, \ldots, c_n) \in D\}.$$

In what follows, we will use the Eq. (1) as our definition of the RGHWs.

Remark 2.3 In view of Lemma 2.2, it is clear that if $C_2 = \{0\}$, then the RGHWs of C_1 w.r.t. C_2 are exactly the generalized Hamming weights of C_1.

2.2 Affine Cartesian codes

In this subsection, we recall the definition of the affine Cartesian codes. Throughout, we will use the convention that the degree of the zero polynomial is -1.

Definition 2.4 Let $d_1 \leq \ldots \leq d_m$ be positive integers and $A_1, \ldots, A_m$ are subsets of $\mathbb{F}_q$ with cardinalities $d_1, \ldots, d_m$ respectively. Denote by $\mathcal{A}$ the cartesian product $\mathcal{A} := A_1 \times \cdots \times A_m$. Note that $|\mathcal{A}| = n := d_1 \cdots d_m$. Further, fix an enumeration $P_1, \ldots, P_n$ of elements in $\mathcal{A}$ and a positive integer $d \leq k := \sum_{i=1}^m (d_i - 1)$. For $d \leq k$, define the subspace

$$S_{\leq d}(\mathcal{A}) := \{f \in \mathbb{F}_q[x_1, \ldots, x_m] : \deg_{x_i} f \leq d_i - 1 \text{ and } \deg f \leq d\}.$$

The map

$$\mathrm{ev} : S_{\leq k}(\mathcal{A}) \to \mathbb{F}_q^{|\mathcal{A}|} \quad \text{by} \quad f \mapsto (f(P_1), \ldots, f(P_n))$$

is a linear map and consequently, for each $d \leq k$, the image $AC_q(d, \mathcal{A}) := \mathrm{ev}(S_{\leq d}(\mathcal{A}))$ is a linear subspace of $\mathbb{F}_q^n$ and is called an *affine cartesian code*.

Henceforth, we will write $A_i := \{\gamma_{i,1}, \ldots, \gamma_{i,d_i}\}$ for $i = 1, \ldots, m$. It is not hard to show that the map ev is injective. This implies that the dimension of $AC_q(d, \mathcal{A})$ is the same as $\dim S_{\leq d}(\mathcal{A})$. As mentioned in the introduction, we are interested in the determination of the RGHWs of an affine Cartesian code w.r.t. a "smaller" affine Cartesian code. More precisely, our goal is to answer the following:

Question 2.5 Let u_1, u_2 be integers satisfying $-1 \leq u_2 < u_1 \leq k$. Determine $M_r(AC_q(u_1, \mathcal{A}), AC_q(u_2, \mathcal{A}))$, for $r \leq \dim AC_q(u_1, \mathcal{A}) - \dim AC_q(u_2, \mathcal{A})$.

To simplify notations, we will denote $M_r(u_1, u_2) := M_r(AC_q(u_1, \mathcal{A}), AC_q(u_2, \mathcal{A}))$ and $\ell := \dim AC_q(u_1, \mathcal{A}) - \dim AC_q(u_2, \mathcal{A})$. We note that if $u_2 = -1$, then $M_r(u_1, u_2)$ are simply the r-th generalized Hamming weights of $AC_q(u_1, \mathcal{A})$. In the recent work [1], the generalized Hamming weights of affine Cartesian codes were completely determined. To answer the above question we introduce the following sets. For an integer $r \leq \ell$, we define,

$$\mathcal{D}_r := \{D \subset AC_q(u_1, \mathcal{A}) \mid D \cap AC_q(u_2, \mathcal{A}) = 0; \dim D = r\}.$$

We endow the set of monomials in $\mathbb{F}_q[x_1, \ldots, x_m]$ with the graded lexicographic order. In the following Lemma we give a necessary and sufficient condition for a subspace of $AC_q(u_1, \mathcal{A})$ to be a member of $\mathcal{D}_r$.

Lemma 2.6 *Let D be a subspace of $AC_q(u_1, \mathcal{A})$ of dimension r. Then $D \in \mathcal{D}_r$ iff there exists $f_1, \ldots, f_r \in S_{\leq k}(\mathcal{A})$ with $D = \mathrm{Span}\{\mathrm{ev}(f_1), \ldots, \mathrm{ev}(f_r)\}$ satisfying the following three conditions:*

(C1) *$f_1, \ldots, f_r$ are linearly independent,*
(C2) *$u_2 < \deg LT(f_i) \leq u_1$ for $i = 1, \ldots, r$,*
(C3) *$LT(f_i) \neq LT(f_j)$ whenever $i \neq j$.*

Consequently, $|\mathrm{Supp}(D)| = n - |Z_{\mathcal{A}}(f_1, \ldots, f_r)|$, where $Z_{\mathcal{A}}(f_1, \ldots, f_r)$ denotes the set of common zeroes of $f_1, \ldots, f_r \in \mathcal{A}$.

Proof It is easy to see that the three conditions are sufficient. To see that they are also necessary, we begin with $D \in \mathcal{D}_r$, and a set of r linearly independent polynomials $f_1, \ldots, f_r$ such that $D = \mathrm{Span}\{\mathrm{ev}(f_1), \ldots, \mathrm{ev}(f_r)\}$. It is clear that the polynomial f_1 satisfies the condition (C2). For $2 \leq s \leq r$, we replace f_s by a linear combination of $f_1, \ldots, f_s$ so that the polynomials $f_1, \ldots, f_s$ satisfy the condition (C3). Clearly the condition (C2) is satisfied for $f_1, \ldots, f_r$. The last assertion follows trivially. □

We now define the following family consisting of sets of r polynomials:

$$\mathcal{C}_r := \{\{f_1, \ldots, f_r\} \mid f_1, \ldots, f_r \text{ satisfy (C1), (C2), (C3)}\}.$$

It follows directly from Lemma 2.6 that

$$M_r(u_1, u_2) = n - \max\{|Z_{\mathcal{A}}(f_1, \ldots, f_r)| : \{f_1, \ldots, f_r\} \in \mathcal{C}_r\}. \tag{2}$$

We have thus shown that the Question 2.5 is equivalent to the following question:

Question 2.7 For integers r, u_1, u_2 and the set $\mathcal{A}$ as above, determine

$$a_r(u_1, u_2, \mathcal{A}) := \max\{|Z_{\mathcal{A}}(f_1, \ldots, f_r)| : \{f_1, \ldots, f_r\} \in \mathcal{C}_r\}.$$

2.3 The footprint bound

In order to answer Question 2.7 we will use the footprint bound. This method of producing upper bounds on generalized Hamming weights of Reed–Muller type codes is dependent on the theory of Gröbner bases and that of affine Hilbert functions. For a comprehensive reading on these notions, the reader is referred to [7]. Most of what follows in this section can be found in [1, Sect. 2]. We provide a somewhat detailed description of what will be used later for the sake of completeness.

Let us denote by S the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_m]$ and for any integer u we define $S_{\leq u} := \{f \in S \mid \deg f \leq u\}$. For any ideal I of S, we define $I_{\leq u} := I \cap S_{\leq u}$. The affine Hilbert function of I, denoted by ${}^a\mathsf{HF}_I$, is defined as

$$ {}^a\mathsf{HF}_I : \mathbb{Z} \to \mathbb{Z} \quad \text{given by} \quad {}^a\mathsf{HF}_I(u) := \dim S_{\leq u} - \dim I_{\leq u}. $$

It is easy to derive that if I and J are ideals of S with $I \subset J$, then for any $u \in \mathbb{Z}$ we have ${}^a\mathsf{HF}_J(u) \leq^a {}^a\mathsf{HF}_I(u)$. For a subset $X \subset \mathbb{F}_q^m$ we define the ideal $I(X)$ to be the ideal of S consisting of polynomials vanishing everywhere in X. For such a subset $X \subset \mathbb{F}_q^m$, we define its affine Hilbert function, denoted by ${}^a\mathsf{HF}_X$, as ${}^a\mathsf{HF}_X :=^a {}^a\mathsf{HF}_{I(X)}$.

Proposition 2.8 (a) [7, Sect. 9.3] *Let $\prec$ be any graded order on S. Then*

(i) *For any ideal I of S, we have ${}^a\mathsf{HF}_{\mathsf{LT}(I)}(u) =^a {}^a\mathsf{HF}_I(u)$.*
(ii) *If I is a monomial ideal of S, then ${}^a\mathsf{HF}_I(u)$ is given by the number of monomials of degree at most u that do not lie in I.*

(b) [19, Lemma 2.1] *If $Y \subset \mathbb{F}_q^m$ is a finite set, then $|Y| =^a {}^a\mathsf{HF}_Y(u)$ for all sufficiently large values of u.*

Similar statements as in the above proposition could also be found, albeit in disguise of footprints, in [9, Corollary 4.5] and in [6, Corollary 2.5]. The above Proposition helps us in finding out an upper bound for the quantity $|\mathsf{Z}_{\mathcal{A}}(f_1, \ldots, f_r)|$ for a given $\{f_1, \ldots, f_r\} \in \mathcal{C}_r$. To this end, we see that the polynomials $g_1, \ldots, g_m \in I(Z_{\mathcal{A}}(f_1, \ldots, f_r))$, where

$$ g_j := \prod_{s=1}^{d_j} (x_j - \gamma_{j,s}) \quad \text{for} \quad j = 1, \ldots, m. $$

At this juncture, it will be useful to assign some notations for the ideals in question. Define

$$ \mathcal{I} := I(Z_{\mathcal{A}}(f_1, \ldots, f_r)) \quad \text{and} \quad \mathsf{LT}(\mathcal{I}) := \text{ the leading term ideal of } \mathcal{I}. $$

Furthermore, we have the monomial ideals:

$$ \mathcal{J} := \langle f_1, \ldots, f_r, g_1, \ldots, g_m \rangle \quad \text{and} \quad \mathcal{J}_{\mathsf{Mon}} := \langle \mathsf{LT}(f_1), \ldots, \mathsf{LT}(f_r), x_1^{d_1}, \ldots, x_m^{d_m} \rangle. $$

It follows trivially from the above discussions that, $\mathcal{J} \subset \mathcal{I}$ and that

$$ \mathcal{J}_{\mathsf{Mon}} \subseteq \mathsf{LT}(\mathcal{J}) \subseteq \mathsf{LT}(\mathcal{I}). \tag{3} $$

Using Proposition 2.8 and Eq. (3) we see that for sufficiently large u,

$$ |\mathsf{Z}_{\mathcal{A}}(f_1, \ldots, f_r)| =^a \mathsf{HF}_{\mathcal{I}}(u) =^a \mathsf{HF}_{\mathsf{LT}(\mathcal{I})}(u) \leq^a \mathsf{HF}_{\mathcal{J}_{\mathsf{Mon}}}(u). \tag{4} $$

Let us write $\mathsf{M} = \{\mu \in S \mid \mu \text{ is a monomial}\}$. It follows from from Proposition 2.8 (a) (ii) that

$$ {}^a\mathsf{HF}_{\mathcal{J}_{\mathsf{Mon}}}(u) = |\{\mu \in \mathsf{M} : \deg \mu \leq u, x_i^{d_i} \nmid \mu, \mathsf{LT}(f_j) \nmid \mu \text{ for } i = 1, \ldots, m \text{ and } j = 1, \ldots, r\}|. $$

Furthermore, if we take $u \geq \sum_{i=1}^m d_i$, then

$$ {}^a\mathsf{HF}_{\mathcal{J}_{\mathsf{Mon}}}(u) = |\{\mu \in \mathsf{M} : \deg_{x_i} \mu \leq d_i - 1, \mathsf{LT}(f_j) \nmid \mu \text{ for } i = 1, \ldots, m \text{ and } j = 1, \ldots, r\}|. $$

We define

$$ \mathsf{M}_{\mathcal{A}} := \{\mu \in \mathsf{M} \mid \deg_{x_i} \mu \leq d_i - 1 \text{ for } i = 1, \ldots, m\}, $$

and given any set of monomials $m_1, \ldots, m_r$, the set of footprints,

$$\mathsf{FP}_{\mathcal{A}}(m_1, \ldots, m_r) := \{\mu \in \mathsf{M}_{\mathcal{A}} : m_i \nmid \mu \text{ for } i = 1, \ldots, r\}.$$

The previous discussions now imply that

$$|\mathsf{Z}_{\mathcal{A}}(f_1, \ldots, f_r)| \leq |\mathsf{FP}_{\mathcal{A}}(\mathsf{LT}(f_1), \ldots, \mathsf{LT}(f_r))|. \tag{5}$$

The upper bound on the number of points on $Z_{\mathcal{A}}(f_1, \ldots, f_r)$ thus obtained from Eq. (5) is referred to as the footprint bound. Indeed,

$$a_r(u_1, u_2, \mathcal{A}) \leq \max\{|\mathsf{FP}_{\mathcal{A}}(\mathsf{LT}(f_1), \ldots, \mathsf{LT}(f_r))| : \{f_1, \ldots, f_r\} \in \mathcal{C}_r\}. \tag{6}$$

In the following subsection, we will introduce some combinatorial notions which will help us to derive the right hand side of the Eq. (6).

2.4 Some combinatorial tools

In this subsection, we will introduce some combinatorial notions that will help us to translate the problem of determining the right hand side of the Eq. (6) to a problem of extremal combinatorics. Let

$$F = \{0, \ldots, d_1 - 1\} \times \cdots \times \{0, \ldots, d_m - 1\}.$$

We have two natural orderings for the elements of F, namely the lexicographic order and the partial order. Let us write

$$(a_1, \ldots, a_m) \prec_{lex} (b_1, \ldots, b_m)$$

if $(a_1, \ldots, a_m)$ is less than $(b_1, \ldots, b_m)$ in lexicographic order, i.e. there exists j with $1 \leq j \leq m$ such that $a_i = b_i$ for all $i < j$ and $a_j < b_j$. Also we will write

$$(a_1, \ldots, a_m) \prec_P (b_1, \ldots, b_m)$$

if and only if $(a_1, \ldots, a_m)$ is less than $(b_1, \ldots, b_m)$ in partial order, i.e. $a_i \leq b_i$ for all $i = 1, \ldots, m$ and for some $j \in \{1, \ldots, n\}$ we have $a_j < b_j$.We write $(a_1, \ldots, a_m) \preceq_{lex} (b_1, \ldots, b_m)$ (resp. $(a_1, \ldots, a_m) \preceq_P (b_1, \ldots, b_m)$) if $(a_1, \ldots, a_m) \prec_{lex} (b_1, \ldots, b_m)$ (resp. $(a_1, \ldots, a_m) \prec_P (b_1, \ldots, b_m)$) or $(a_1, \ldots, a_m) = (b_1, \ldots, b_m)$. We have a bijection

$$\phi : \mathsf{M}_{\mathcal{A}} \to F \text{ given by } x_1^{a_1} \cdots x_m^{a_m} \mapsto (a_1, \ldots, a_m).$$

It is clear that for $\mu_1, \mu_2 \in \mathsf{M}_{\mathcal{A}}$, we have $\mu_1 \mid \mu_2$ if and only if $\phi(\mu_1) \preceq_P \phi(\mu_2)$. Now for $\mathbf{a} = (a_1, \ldots, a_m) \in F$, we define $\deg(\mathbf{a}) := a_1 + \cdots + a_m$. Let us introduce some subsets of F consisting of elements satisfying certain degree constraints: for any integer u, define

$$F_u := \{\mathbf{a} \in F : \deg(\mathbf{a}) = u\} \quad \text{and} \quad F_{\leq u} := \{\mathbf{a} \in F : \deg(\mathbf{a}) \leq u\}.$$

On a similar note, for integers u_1, u_2 satisfying $u_2 < u_1$, we define

$$F_{u_2}^{u_1} := \{\mathbf{a} \in F : u_2 < \deg(\mathbf{a}) \leq u_1\}.$$

Given a subset $S \subset F$, we define the shadow (resp. footprint) of S in F, denoted by $\nabla(S)$ (resp. $\Delta(S)$) as follows:

$$\nabla(S) := \{\mathbf{b} \in F \mid \mathbf{a} \preceq_P \mathbf{b} \text{ for some } \mathbf{a} \in S\} \text{ and } \Delta(S) := F \setminus \nabla(S).$$

For an integer u, we define $\Delta_u(S) := \Delta(S) \cap F_u$ and $\nabla_u(S) := \nabla(S) \cap F_u$. It now follows from Eq. (6) that

$$a_r(u_1, u_2, \mathcal{A}) \leq \max\{|\Delta(S)| : S \subset F_{u_2}^{u_1}, |S| = r\}. \tag{7}$$

In the subsequent section, we will derive the exact value of the right hand side in the above inequality. Before concluding this section, we remark that the field $\mathbb{F}_q$ does not play an essential role as long as we are interested in computing the quantity $a_r(u_1, u_2, \mathcal{A})$. The inequalities (6) and (7) continue to hold even if we replace $\mathbb{F}_q$ by an arbitrary field having at least d_m elements.

3 Result from combinatorics

Motivated from the discussion in the last section, we now investigate the following question.

Question 3.1 Fix integers u_1, u_2 and r with $-1 \leq u_2 < u_1 \leq k$. Denote by $\mathcal{F}_r$, the family of subsets of $F_{u_2}^{u_1}$ of cardinality r. Determine $\max\{|\Delta(S)| : S \in \mathcal{F}_r\}$.

We remark that if $d_1 = d_2 = \cdots = d_m = q$, then the answer to this question is known in various cases:

(1) for $u_2 = -1$, this question corresponds to the determination of the GHWs of the Reed–Muller codes, which was solved by Heijnen and Pellikaan in [15].
(2) in general, without any constraint on u_2, the question corresponds to the determination of the RGHWs of the Reed–Muller codes, and as mentioned before, this question was answered by Geil and Martin in [11].

Furthermore, in the general situation with $d_1 \leq \cdots \leq d_m$, this problem was solved in [1] in the case $u_2 = -1$ in order to determine the GHWs of the affine Cartesian codes. In order to proceed, we first introduce the following two notations:

(a) For and integer u and a subset $S \subset F_u$, we define $L(S)$ to be the set consisting of the first $|S|$ elements of F_u in descending lexicographic order.
(b) For integers u_1, u_2 with $-1 \leq u_2 < u_1 \leq k$ and a subset $S \subset F_{u_2}^{u_1}$, we define $N(S)$ to be the set consisting of the first $|S|$ elements of $F_{u_2}^{u_1}$ in descending lexicographic order.

The following classical Theorem, due to Clements and Lindström, will play an instrumental role in the sequel.

Theorem 3.2 [5, Corollary 1] *Let $u < k$ and $S \subseteq F_u$. Then*

$$\nabla_{u+1}(L(S)) \subseteq L(\nabla_{u+1}(S)).$$

The following is an easy corollary of the Theorem 3.2.

Corollary 3.3 *For integers u, v with $u \leq v \leq k$ and $S \subset F_u$, we have*

(a) [1, Corollary 3.2] $\nabla_v(L(S)) \subseteq L(\nabla_v(S))$ *and thus,* $|\nabla_v(L(S))| \leq |\nabla_v(S)|$.
(b) [1, Corollary 3.3] $|\nabla(L(S))| \leq |\nabla(S)|$.

In order to prove our main results, we will also need the following lemma that can be found in [1, Lemma 3.4 and Remark 3.5].

Lemma 3.4 *Fix integers u, v with $u < v \leq k$ and an element $\boldsymbol{y} \in F_v$. If $\boldsymbol{a}_{\boldsymbol{y}} := \max_{lex}\{\boldsymbol{f} \in F_u : \boldsymbol{f} \preceq_{lex} \boldsymbol{y}\}$, then $\boldsymbol{a}_{\boldsymbol{y}} \preceq_P \boldsymbol{y}$.*

The following two lemmas are motivated from their analogues [1, Lemmas 3.6 and 3.7]. We include the proofs for the sake of completeness.

Lemma 3.5 *Let u, u_1, u_2 be integers satisfying $-1 \le u_2 < u \le u_1 \le k$. Let $N(r)$ denote the first r elements of $F_{u_2}^{u_1}$ in descending lexicographic order. If $N_u := N(r) \cap F_u$ and $r_u := |N_u|$, then*

$$\nabla_{u_1}(N_u) \subseteq N_{u_1} \subseteq \nabla_{u_1}(N_u^*),$$

where N_u^* consists of the first $r_u + 1$ elements of F_u in descending lexicographic order.

Proof The result is trivially true if $u = u_1$. So we may assume that $u < u_1$. Let $\mathbf{y} \in \nabla_{u_1}(N_u)$. Then there exists $\mathbf{x} \in N_u$ such that $\mathbf{x} \preceq_P \mathbf{y}$. Consequently $\mathbf{x} \preceq_{lex} \mathbf{y}$. Since $\mathbf{x} \in N(r)$ and $\mathbf{x} \preceq_{lex} \mathbf{y}$, we have $\mathbf{y} \in N(r)$. Since $\mathbf{y} \in F_{u_1}$, we have $\mathbf{y} \in N(r) \cap F_{u_1} = N_{u_1}$.

Now let $\mathbf{y} \in N_{u_1}$. Define $\mathbf{a} := \max_{lex}\{\mathbf{f} \in F_u : \mathbf{f} \preceq_{lex} \mathbf{y}\}$. From Lemma 3.4, we obtain $\mathbf{a} \preceq_P \mathbf{y}$. If $\mathbf{a} \in N_u$, then $\mathbf{a} \in N_u^*$, which proves the assertion. So we may assume that $\mathbf{a} \notin N_u$. Clearly, the set N_u consists of the first r_u elements of F_u in descending lexicographic order. If we write $N_u^* = \{\mathbf{f}_1, \ldots, \mathbf{f}_{r_u+1}\}$, then $\mathbf{a} \preceq_{lex} \mathbf{f}_{r_u+1}$. If $\mathbf{a} = \mathbf{f}_{r_u+1}$, then $\mathbf{a} \in N_u^*$, and the assertion follows. Now suppose, if possible, that $\mathbf{a} \prec_{lex} \mathbf{f}_{r_u+1}$. The maximality of $\mathbf{a}$ implies that $\mathbf{y} \prec_{lex} \mathbf{f}_{r_u+1}$. Since $\mathbf{y} \in N(r)$, it follows that $\mathbf{f}_{r_u+1} \in N(r)$ and hence $\mathbf{f}_{r_u+1} \in N_u$. This contradicts $|N_u| = r_u$. This completes the proof. □

Lemma 3.6 *With notations as in Lemma 3.5 and $u_2 < u_1 - 1$, we have*

$$|\nabla(N(r))| = r - |N_{u_1}| + |\nabla(N_{u_1})|.$$

Proof It follows from Lemma 3.5 that,

$$\bigcup_{u_2 < u \le u_1} \nabla_{u_1}(N_u) \subset N_{u_1}. \tag{8}$$

This implies,

$$\begin{aligned} |\nabla(N(r))| &= |\nabla(N(r)) \cap F_{<u_1}| + |\nabla(N(r)) \cap F_{\ge u_1}| \\ &= |\nabla(N(r) \setminus N_{u_1}) \cap F_{<u_1}| + |\nabla(N_{u_1})|. \end{aligned}$$

Note that, $N(r) \setminus N_{u_1}$ consists of the first $r - |N_{u_1}|$ elements of $F_{u_2}^{u_1-1}$ in descending lexicographic order. We obtain by applying (8) to $N(r) \setminus N_{u_1}$ (on $F_{u_2}^{u_1-1}$) that $\nabla_{u_1-1}(N(r) \setminus N_{u_1})) \subset N_{u_1-1}$. Also, $N_{u_1-1} \subset N(r) \setminus N_{u_1}$. This implies that $\nabla_{u_1-1}(N(r) \setminus N_{u_1}) = N_{u_1-1}$. Repeating the argument iteratively we deduce that,

$$\nabla_u(N(r) \setminus N_{u_1}) = N_u \quad \text{for all} \quad u_2 < u \le u_1 - 1.$$

Consequently, $\nabla(N(r) \setminus N_{u_1}) \cap F_{<u_1} = N(r) \setminus N_{u_1}$, which proves the lemma. □

We are now ready to state and prove the main theorem of this section. This is a generalization of [1, Theorem 3.8]. Further special cases, when $d_1 = \cdots = d_m = q$, appear as [21, Lemma 6], [15, Theorem 5.7] and [11, Lemma 4.6].

Theorem 3.7 *Let u_1, u_2, u, r be integers with $-1 \le u_2 < u_1 \le k$ and let $S \subseteq F_{u_2}^{u_1}$ with $|S| = r$. Then $|\nabla(N(r))| \le |\nabla(S)|$. In particular, given any $S \in \mathcal{F}_r$, we have $|\Delta(S)| \le |\Delta(N(r))|$. Consequently,*

$$|\Delta(N(r)| = \max\{|\Delta(S)| : S \in \mathcal{F}_r\}.$$

Proof For $u_2 < u \leq u_1$, define $S_u := S \cap F_u$ and $N_u := N(r) \cap F_u$. When $u_2 = u_1 - 1$, then the assertion follows directly from Corollary 3.3 (b). Henceforth, we will always assume that $u_2 < u_1 - 1$. We distinguish the proof in two cases:

Case 1: Suppose that $|S_{u_1}| \geq r_{u_1}$. Then $|S_{u_1}| = r_{u_1} + \alpha$ for some $\alpha \geq 0$. We may write $S_{u_1} = S' \cup S''$, where S' denotes the first r_{u_1} elements of S in descending lexicographic order and $S'' = S \setminus S'$. It follows easily that $|S''| = \alpha$ and that S'' is disjoint from $\nabla(S)$ and $\nabla(N_{u_1})$. By applying Corollary 3.3 (b) to S', we see that $|\nabla(S')| \geq |\nabla(N_{u_1})|$. This shows that $|\nabla(S_{u_1})| \geq |\nabla(N_{u_1})| + \alpha$. We note that,

$$\begin{aligned} |\nabla(S)| &= |\nabla_{<u_1}(S)| + |\nabla_{\geq u_1}(S)| \\ &\geq |\nabla_{<u_1}(S)| + |\nabla(S_{u_1})| \\ &\geq |S \cap F_{<u_1}| + |\nabla(S_{u_1})| \\ &= r - |S_{u_1}| + |\nabla(S_{u_1})|. \end{aligned} \tag{9}$$

This gives

$$|\nabla(S)| \geq r - |S_{u_1}| + |\nabla(S_{u_1})| \geq r - r_{u_1} - \alpha + |\nabla(N_{u_1})| + \alpha = |\nabla(N(S))|.$$

The last equality follows from Lemma 3.6 and the proof is complete in this case. **Case 2:** Now suppose that $|S_{u_1}| < r_{u_1}$. Since $|S| = r = |N(r)|$, there exists and integer u with $u_2 < u < u_1$ such that $|S_u| > |N_u|$ and consequently, $|N_u^*| \leq |S_u|$. By Lemma 3.5 and Corollary 3.3 (a) we have $|N_{u_1}| \leq |\nabla_{u_1}(N_u^*)| \leq |\nabla_{u_1}(S_u)|$. Thus,

$$\begin{aligned} |\nabla(S)| &\geq r - |S_{u_1}| + |\nabla_{\geq u_1}(S)| \quad \text{(follows from (9))} \\ &> r - |N_{u_1}| + |\nabla_{\geq u_1}(S_u)| \\ &= r - |N_{u_1}| + |\nabla(\nabla_{u_1}(S_u))| \\ &\geq r - |N_{u_1}| + |\nabla(N_{u_1})| = |\nabla(N(S))|. \end{aligned}$$

The inequality $|\nabla(\nabla_{u_1}(S_u))| \geq |\nabla(N_{u_1})|$ follows from Corollary 3.3 (b) and the last equality follows from Lemma 3.6. The last two assertions are now obvious. □

In order to answer Question 3.1 we must now determine $|\nabla(N(r))|$. To proceed we will need the following Lemma that was proved in [1, Lemma 4.2].

Lemma 3.8 [1, Lemma 4.2] *Let $d > 0$ be an integer and $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r$ be the first r elements of $F_{\leq d}$ in descending lexicographic order. Then,*

$$\nabla(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r) = \{\boldsymbol{a} \in F : \boldsymbol{a}_r \preceq_{lex} \boldsymbol{a}\}.$$

Moreover, if $\boldsymbol{a}_r = (a_{r,1}, \ldots, a_{r,m})$ then

$$|\nabla(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r)| = d_1 \cdots d_m - \sum_{i=1}^{m} a_{r,i} \prod_{j=i+1}^{m} d_j.$$

The following Proposition, where we compute the $|\nabla(N(r))|$ completes our pursuit of answering Question 3.1.

Proposition 3.9 *Let u_1, u_2, r be as above. Assume that $N(r) := \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r\}$. Suppose $\boldsymbol{a}_r$ is the s-th element of $F_{\leq u_1}$ in descending lexicographic order. Then,*

$$|\nabla(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r)| = d_1 \cdots d_m - \sum_{i=1}^{m} a_{r,i} \prod_{j=i+1}^{m} d_j - s + r.$$

Proof Let us denote by $M_{u_1}(s)$ the first s elements of $F_{\leq u_1}$ in descending lexicographic order. Clearly, $\mathbf{a}_i \in M_{u_1}(s)$ for $i = 1, \ldots, r$. It is easy to see that

$$\nabla(\mathbf{a}_1, \ldots, \mathbf{a}_r) = \nabla(M_{u_1}(s)) \setminus \left(M_{u_1}(s) \setminus N(r)\right),$$

which proves that

$$|\nabla(\mathbf{a}_1, \ldots, \mathbf{a}_r)| = |\nabla(M_{u_1}(s))| - (s - r).$$

The assertion now follows from Lemma 3.8 by noting that $\mathbf{a}_r$ is the s-th element of $M_{u_1}(s)$ in descending lexicographic order. □

We have thus answered the Question 3.1 completely and we note it down as the following corollary.

Corollary 3.10 *Fix integers u_1, u_2 and r with $-1 \leq u_2 < u_1 \leq k$. Denote by $\mathcal{F}_r$, the family of subsets of $F_{u_2}^{u_1}$ of cardinality r. Then*

$$\max\{|\Delta(S)| : S \in \mathcal{F}_r\} = \sum_{i=1}^{m} a_{r,i} \prod_{j=i+1}^{m} d_j + s - r,$$

where $(a_{r,1}, \ldots, a_{r,m})$ is the r-th element of $F_{u_2}^{u_1}$ and s-th element of $F_{\leq u_1}$ in descending lexicographic order. In particular,

(a) $a_r(u_1, u_2, \mathcal{A}) \leq \sum_{i=1}^{m} a_{r,i} \prod_{j=i+1}^{m} d_j + s - r$ *and*

(b) $M_r(u_1, u_2) \geq d_1 \cdots d_m - \sum_{i=1}^{m} a_{r,i} \prod_{j=i+1}^{m} d_j - s + r.$

Proof The first assertion follows from Theorem 3.7 and Proposition 3.9. The assertion (a) follows from Eq. (6) and we now derive (b) as a consequence of Eq. (2). □

In the following and the last section of this article, we will produce a set $\{f_1, \ldots, f_r\} \in \mathcal{C}_r$ for which the upper bound for $a_r(u_1, u_2, \mathcal{A})$ given in the Corollary 3.10 is attained.

4 Maximal family of polynomials and the relative generalized Hamming weights of affine Cartesian codes

As mentioned before, we now construct a family of polynomials $\{f_1, \ldots, f_r\} \in \mathcal{C}_r$ such that $|\mathrm{Z}_{\mathcal{A}}(f_1, \ldots, f_r)|$ attains the upper bound for $a_r(u_1, u_2, \mathcal{A})$ as obtained in Corollary 3.10. We call such a family of polynomials as a maximal family. First, recall that, $A_i = \{\gamma_{i,1}, \ldots, \gamma_{i,d_i}\}$ for $i = 1, \ldots, m$.

Definition 4.1 For $\mathbf{b} = (b_1, \ldots, b_m) \in F$ define the polynomial,

$$f_{\mathbf{b}} = \prod_{i=1}^{m} \prod_{j=1}^{b_i} (x_i - \gamma_{i,j}).$$

We may note that $\deg f_{\mathbf{b}} = b_1 + \cdots + b_m$ and with respect to the graded lexicographic order the leading term of $f_{\mathbf{b}}$ is given by $\mathsf{LT}(f_{\mathbf{b}}) = x_1^{b_1} \cdots x_m^{b_m}$. We further observe that, We define a map $\psi : \mathcal{A} \to F$ given by $(\gamma_{1,i_1}, \ldots, \gamma_{m,i_m}) \mapsto (i_1 - 1, \ldots, i_m - 1)$. The map ψ is a bijection. It follows easily that for $\gamma \in \mathcal{A}$,

$$f_{\mathbf{b}}(\gamma) \neq 0 \iff \psi(\gamma) \in \nabla(\mathbf{b}) \tag{10}$$

We have the following proposition which is an analogue of [1, Proposition 4.5].

Proposition 4.2 *Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_r$ be the first r elements of $F_{u_2}^{u_1}$ in descending lexicographic order and suppose that $\boldsymbol{a}_r$ is the s-th element of $F_{\leq u_1}$ in descending lexicographic order. Then,*

$$|\mathrm{Supp}(f_{\boldsymbol{a}_1}, \ldots, f_{\boldsymbol{a}_r})| = d_1 \cdots d_m - \sum_{i=1}^{m} a_{r,i} \prod_{j=i+1}^{m} d_j - s + r,$$

where $\boldsymbol{a}_r = (a_{r,1}, \ldots, a_{r,m})$ and $\mathrm{Supp}(f_{\boldsymbol{a}_1}, \ldots, f_{\boldsymbol{a}_r}) = \mathcal{A} \setminus Z_{\mathcal{A}}(f_{\boldsymbol{a}_1}, \ldots, f_{\boldsymbol{a}_r})$.

Proof It follows from Eq. (10) that $\gamma \in \mathrm{Supp}(f_{\mathbf{a}_1}, \ldots, f_{\mathbf{a}_r})$ if and only if $\psi(\gamma) \in \Delta(\mathbf{a}_1, \ldots, \mathbf{a}_r)$. Thus, $|\mathrm{Supp}(f_{\mathbf{a}_1}, \ldots, f_{\mathbf{a}_r})| = |\nabla(\mathbf{a}_1, \ldots, \mathbf{a}_r)|$. Since $\mathbf{a}_1, \ldots, \mathbf{a}_r$ are the first r elements of $F_{u_1}^{u_2}$ in descending lexicographic order we see that,

$$|\mathrm{Supp}(f_{\mathbf{a}_1}, \ldots, f_{\mathbf{a}_r})| = |\nabla(\mathbf{a}_1, \ldots, \mathbf{a}_r)| = d_1 \cdots d_m - \sum_{i=1}^{m} a_{r,i} \prod_{j=i+1}^{m} d_j - s + r,$$

where the last equality follows from Proposition 3.9. This completes the proof. □

Finally we may state the main result of this paper where we compute all the RGHWs of an affine Cartesian code with respect to a smaller affine Cartesian code.

Theorem 4.3 *Fix integers u_1, u_2 with $-1 \leq u_2 < u_1 \leq \sum_{i=1}^{m}(d_i - 1)$. Let $AC_q(u_1, \mathcal{A})$ and $AC_q(u_2, \mathcal{A})$ denote the corresponding affine Cartesian codes. For any integer $1 \leq r \leq \ell := \dim AC_q(u_1, \mathcal{A}) - \dim AC_q(u_2, \mathcal{A})$, the r-th RGHW of $AC_q(u_1, \mathcal{A})$ with respect to $AC_q(u_2, \mathcal{A})$, denoted by $M_r(u_1, u_2)$ is given by*

$$M_r(u_1, u_2) = d_1 \cdots d_m - \sum_{i=1}^{m} a_{r,i} \prod_{j=i+1}^{m} d_j - s + r,$$

where $(a_{r,1}, \ldots, a_{r,m})$ is the r-th element of $F_{u_2}^{u_1}$ and s-th element of $F_{\leq u_1}$ in descending lexicographic order.

Proof The result follows from Corollary 3.10 and Proposition 4.2. □

Acknowledgements Open Access funding provided by UiT The Arctic University of Norway. The author expresses his gratitude to Olav Geil for pointing out this problem, Peter Beelen for some enlightening discussions on these topics, and Trygve Johnsen for his careful reading of the manuscript and several comments. The author also thanks the reviewers for their careful reading of the article and their comments. The funding was provided by Norges Forskningsråd (Grant No. 280731).

References

1. Beelen P., Datta M.: Generalized Hamming weights of affine cartesian codes. Finite Fields Appl. **51**, 130–145 (2018).
2. Beelen P., Datta M., Ghorpade S.R.: Vanishing ideals of projective spaces over finite fields and a projective footprint bound. Acta Math. Sin. **35**(1), 47–63 (2019).
3. Carvalho C.: On the second Hamming weight of some Reed-Muller type codes. Finite Fields Appl. **24**, 88–94 (2013).
4. Carvalho C., Neumann V.G.L.: On the next-to-minimal weight of affine cartesian codes. Finite Fields Appl. **44**, 113–134 (2017).
5. Clements G.F., Lindström B.: A generalization of a combinatorial theorem of Macaulay. J. Comb. Theory **7**, 230–238 (1969).
6. Cox D.A., Little J., O'Shea D.: Using Algebraic Geometry. Graduate Texts in Mathematics, 2nd edn. Springer, New York (2005).
7. Cox D.A., Little J., O'Shea D.: Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra. Undergraduate Texts in Mathematics, 4th edn. Springer, Cham (2015).
8. Fitzgerald J., Lax R.F.: Decoding affine variety codes using Gröbner bases. Des. Codes Cryptogr. **13**, 147–158 (1998).
9. Geil O.: Evaluation Codes from an Affine Variety Code Perspective, Chapter 2 in Advances in Algebraic Geometry Codes, Series on Coding Theory and Cryptology, vol. 5. World Scientific Publishing Co. Pvt. Ltd., Singapore (2008).
10. Geil O., Høholdt T.: Footprints or generalized Bezout's theorem. IEEE Trans. Inf. Theory **46**, 635–641 (2000).
11. Geil O., Martin S.: Relative generalized Hamming weights of q-ary Reed-Muller codes. Adv. Math. Commun. **11**(3), 503–531 (2017).
12. Geil O., Thomsen C.: Weighted Reed-Muller codes revisited. Des. Codes Cryptogr. **66**, 195–220 (2013).
13. Gonzalez-Sarabia M., Martínez-Bernal J., Villarreal R.H., Vivares C.E.: Generalized minimum distance functions. J. Algebraic Comb. **50**(3), 317–346 (2019).
14. Høholdt T.: On (or in) Dick Blahut's Footprint, Codes, Curves and Signals, pp. 3–9. Kluwer, Norwell (1998).
15. Heijnen P., Pellikaan R.: Generalized Hamming weights of q-ary Reed-Muller codes. IEEE Trans. Inf. Theory **44**, 181–196 (1998).
16. Liu Z., Chen W., Luo Y.: The relative generalized Hamming weight of linear q-ary codes and their subcodes. Des. Codes Cryptogr. **48**, 111–123 (2008).
17. López H.H., Rentería-Márquez C., Villarreal R.H.: Affine cartesian codes. Des. Codes Cryptogr. **71**(1), 5–19 (2014).
18. Luo Y., Mitrpant C., Vinck A.H., Chen K.: Some new characters on the wire-tap channel of type II. IEEE Trans. Inf. Theory **51**, 1222–1229 (2005).
19. Nie Z., Wang A.Y.: Hilbert functions and the finite degree Zariski closure in finite field combinatorial geometry. J. Combin. Theory Ser. A **134**, 196–220 (2015).
20. Núñez-Betancourt L., Pitones Y., Villarreal R.H.: Footprint and minimum distance functions. Commun. Korean Math. Soc. **33**(1), 85–101 (2018).
21. Wei V.K.: Generalized Hamming weights for linear codes. IEEE Trans. Inf. Theory **37**, 1412–1418 (1991).